EXHIBIT A

Dr. Matthew Green – Updated Expert Disclosure

- As set forth in more detail in his curriculum vitae, which is attached as Exhibit A-1,[1] Dr. Green is an expert in cryptography and blockchain technology (including cryptocurrencies). Dr. Green is an associate professor of computer science and member of the Johns Hopkins University Information Security Institute, and is a nationally recognized expert on applied cryptography, cryptographic engineering, information security and online privacy. He is one of the creators of the privacy-preserving cryptocurrency blockchain Zcash. Dr. Green has been engaged with cryptography since approximately 1999 and blockchain technology (including cryptocurrencies) since approximately 2011. From 2005 until 2011, Dr. Green was a partner of an information security evaluation firm, which was known as Independent Security Evaluators. His education and his professional qualifications to offer the below-described opinions are set forth in detail in his curriculum vitae. His curriculum vitae lists his publications for the prior ten years and he has not testified in the past four years as an expert at trial or in a deposition.

- In forming his opinions, Dr. Green has relied upon his education, knowledge, experience, and training in cryptography and blockchain technology (including cryptocurrencies), computer science, information security, and online privacy, including financial security and privacy. As part of the basis for his opinions, Dr. Green has also relied upon his own research in these fields, as well as his attendance at and participation in blockchain/cryptocurrency conferences, as well as other technology-related conferences on subjects like cryptography and information security. His testimony will also be based on his review of publicly available information and documentation regarding venture capital fundraising (including reviewing Crunchbase), Bitcoin and Ethereum (including their blockchain explorers, source code, and GitHub documentation and review of such public sources like www.bitcointalk.org and www.ethereum.org), as well as Tornado Cash (including its source code and GitHub documentation) and other cryptocurrency privacy tools (and cryptocurrency blockchains), and his experience using Bitcoin, Ethereum, and Tornado Cash. His testimony will also be based on his experience advising and participating in cryptocurrency-related projects, which included meeting and conferring with venture capitalists, software developers, regulators, and law enforcement.

- Dr. Green is expected to offer background testimony on online cryptography, open-source software (including the role of GitHub, a Microsoft company that operates a publicly available software depository/database), cryptocurrency blockchains/protocols (e.g., Bitcoin, Ethereum, and Tornado Cash), how BTC and ETH are the native cryptocurrencies of Bitcoin and Ethereum (respectively), the Tornado Cash protocol (including how its smart contracts work and the role of ETH and TORN (the Tornado Cash token)), the history of privacy in electronic payment and networking systems (e.g., Virtual Private Networks ("VPNs")), the history of cryptocurrency privacy (including other privacy-related cryptocurrency blockchains like Zcash and its native token ZEC),

[1] This references the curriculum vitae provided to the government on March 5, 2025.

and the history of online information privacy and security, including financial privacy and security.

- Dr. Green is expected to opine the following. Online privacy is important because the Internet exposes a user's personal information which can be exploited. For example, it can be re-sold by data brokers, used to market products to the user, and obtained by bad actors (who steal identities or worse). The Internet exposes personal information that can be exploited, such as the user's location, purchases, financial transactions, social graphs, and nearby digital devices.

- Dr. Green is expected to opine that there are online tools that can be used to protect users' online privacy, and to explain how some of them operate. These tools include Transport Layer Security (which can, for example, protect web browsing), messaging encryption, VPNs (which can protect the user's Internet Protocol ("IP") address), and Apple Pay (which can protect credit card numbers).

- Dr. Green is expected to offer background testimony about online financial privacy and to opine that individuals and entities can be subject to exploits by bad actors. Traditional financial institutions (known as "TradFi") are centralized, with a user's banking information (transactions, balance, etc.) known to that user's bank, but not to the general public (including online) unless the user chooses to reveal it themselves or it is stolen. Traditional financial institutions, like banks, use many security tools to protect a user's online information. That said, there have been many exploits by bad actors (e.g., hacks) of traditional financial institutions, like credit reporting agencies, that result in bad actors obtaining users' personal information.

- Dr. Green is expected to offer background testimony about the following. How cryptocurrency blockchains work (e.g., Bitcoin and Ethereum), and that many are not centrally controlled (e.g., do not operate on a centralized computer(s)). Neither Bitcoin nor Ethereum keeps a user's account balance on a centrally controlled computer. Both consist of large networks that anyone can participate in. The Ethereum Foundation website, for example, provides instructions for how to set up an Ethereum node. Anyone who wants to join such a network (e.g., Bitcoin and Ethereum) can download and view every single transaction ever.

- Dr. Green is expected to opine the following. That cryptocurrency blockchains often lack privacy (e.g., Bitcoin and Ethereum), and to explain why this is so. With Bitcoin and Ethereum, every single node operator sees every transaction. This can reveal the sender and recipient "wallet addresses" (which are similar to bank account numbers) and the amount. Bitcoin and Ethereum addresses do not contain a name (they are alphanumeric), but they often can be linked back to a user through various methods (e.g., self-identification, transaction analysis, or a computer hack) and in some instances it is publicly known who owns certain wallet addresses (e.g., Vitalik Buterin, the founder of Ethereum). Some users post their wallet address(es) or "ENS name" on social media. Dr. Green will explain how Ethereum transactions work, including how ETH moves wallet to wallet and how to trace its movement.

- Dr. Green is expected to offer background testimony about cryptocurrency blockchain explorers, including those for Bitcoin and Ethereum, and how they work. There are special websites called "blockchain explorers" that allow the public to see all transactions made on a cryptocurrency blockchain (e.g., www.etherscan.io for Ethereum and www.blockstream.info for Bitcoin). Dr. Green is also expected to provide examples of tracing transactions in BTC and ETH on blockchain explorers.

- Dr. Green is expected to opine the following. That there are various risks associated with cryptocurrency blockchains that lack privacy (e.g., Bitcoin and Ethereum). As their native cryptocurrencies have become more widely adopted (e.g., BTC and ETH) and often part of mainstream financial services offerings, privacy concerns and risks have only become heightened. For example, bad actors can (1) hack into a user's wallet address and steal cryptocurrency; (2) target a user for fraud; and (3) extort a user and physically hurt that user and others, like their family. These concerns and risks are not theoretical, and there are instances of dangerous gangs engaged in cryptocurrency-stealing home invasions and people being threatened, harmed, and even kidnapped by bad actors attempting to take their cryptocurrency.

- Dr. Green is expected to opine that there are many privacy-preserving cryptocurrency blockchains (including Zcash and Monero) and protocols (like Railgun) and to explain how they operate.

- Dr. Green is expected to opine the following. How one can make transactions on the Bitcoin and Ethereum networks more private, including explaining zero knowledge proofs. One method to make cryptocurrency blockchain transactions private is to encrypt the transactions so they are not publicly visible, and to use zero knowledge proofs to ensure the transactions are valid. Software code that effectuates this method is legal and widely distributed. The general purpose of such a privacy tool is to enable its user to move cryptocurrency from one wallet address to another wallet address without a publicly visible tie. And he will explain that many in the Ethereum community, including Mr. Buterin, have publicly sought the creation of such privacy tools for Ethereum.

- Dr. Green is expected to opine the following. Cryptocurrency privacy tools and privacy-preserving cryptocurrency blockchains are designed to protect legitimate users. Such privacy tools and privacy-preserving cryptocurrency blockchains have been funded by respected venture capitalists, including ones based in the U.S., and by people, including in the U.S., who do not want to promote or engage in criminal activity. Such cryptocurrency privacy tools and privacy-preserving cryptocurrency blockchains are a necessary and logical outgrowth of the legitimate need for online financial privacy.

- Dr. Green is expected to opine the following. Tornado Cash helps provide privacy to legitimate Ethereum users. This will include a discussion of how Tornado Cash operated (from its inception in 2019 through in or about August 8, 2022), and how a user engaged with Tornado Cash, whether through the web-based user interface (referenced often as the "UI") or not, and what can and cannot be seen on an Ethereum blockchain explorer (e.g., www.etherscan.io). This will also include a discussion of UI design, and why UI design

for Tornado Cash or a similar privacy project would also be designed to achieve user privacy.

- Dr. Green is expected to opine the following. U.S.-based companies and software developers generally do not post software tools, including cryptocurrency privacy tools and privacy-preserving cryptocurrency blockchains on GitHub intending for them to be used in criminal activity; rather, they intend for them to be used for legitimate purposes. Software tools designed for criminal activity are often posted and advertised by their creators on dark markets and/or not made publicly available. U.S.-based venture capital firms generally do not invest in companies that intend to promote or facilitate criminal activity.

In addition to the bases set forth above, Dr. Green has also reviewed and relied on the following items:

- Indictment and Filings – *United States v. Storm*
- Government Expert Disclosures – *United States v. Storm*

Approval and Signature

I approve the disclosure of my qualifications, anticipated opinions, and bases for such opinions, as set forth above.

DocuSigned by:
39CE6364BB5241C...
Dr. Matthew Green